IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS 11 PERKINS AVE, UNIT 1, HAMPTON, NEW HAMPSHIRE 03842 AND THE PERSON OF ANTHONY SILVA	Case No. 22-mj-44-AJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Postal Inspector Stephen Riggins, being duly sworn, hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search (1) the premises known as 11 Perkins Ave, Unit 1, Hampton, NH (hereinafter the "Subject Residence") and (2) the person of Anthony SILVA (hereafter "SILVA"), for the documents, records, cellular telephones and electronic devices described herein. As set forth below, there is probable cause to believe that these locations and items contain evidence and are instrumentalities of violations pertaining to 18 U.S.C. § 1343 (Wire Fraud); 42 U.S.C. § 408(a)(7)(B) (False Representation of a Social Security Number); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1344 (Bank Fraud); and associated conspiracy offenses (collectively, the "Subject Offenses").

2. I am a Postal Inspector with the U.S. Postal Inspection Service ("USPIS") assigned to the Manchester, NH office. I have been employed as a Postal Inspector since May 2013. In preparation for this assignment, and as part of my continued education, I have successfully completed law enforcement training, including formal courses and training exercises. I have participated in many aspects of federal investigations including, but not limited

to: subject, victim, and witness interviews; analysis of telephone and financial records; and assisting with the preparation and execution of arrest and/or search warrants. As a federal agent, I am authorized to investigate violations of the laws of the United States. As a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. This matter has two distinct components. The first concerns potential fraud involving Citizens Bank and the Vermont Department of Labor. The second concerns potential fraud involving American Express (AMEX).

Fraud Involving Citizens Bank and the Vermont Department of Labor

5. In June 2021, Goffstown Police began investigating a fraud case pertaining to an individual known by "Ryan Amaro." "Amaro" was evicted from his apartment at 731 Mast Road, #1L, Goffstown, NH 03045. When the landlord, W.Z., later made entry into the apartment to begin cleaning and identifying repairs, she found a large quantity of bank cards, a cash counting machine, and Identification Documents (IDs) in multiple names including Anthony Silva. At this time, W.Z. called her attorney and explained her concern that her former tenant was committing fraud. Her lawyer advised W.Z. to leave all items and contact the police.

6. Goffstown Police responded to the apartment and took custody of 96 bank cards and two driver's licenses. Approximately 32 cards were associated with Citizens Bank.

7. On June 24, 2021, law enforcement agents went to the 731 Mast Road property for a civil standby for "Ryan Amaro" to retrieve his belongings from Apartment 1L. A 2010 Lincoln MKZ, bearing NH license plate 4885883 (hereinafter the "Subject Vehicle") arrived and

parked in the driveway, followed by a U-Haul moving truck. Law enforcement agents recognized the driver of the Subject Vehicle as SILVA. When asked by law enforcement to voluntarily show identification or provide a date of birth, SILVA declined. He then left.

8. The driver of the U-Haul, R.J., then also identified "Ryan Amaro" as SILVA.

9. Law enforcement confirmed that SILVA had rented the U-Haul for the civil standby. U-Haul records showed that SILVA submitted a license with his photo as part of the rental agreement.

10. Law enforcement subsequently brought the Citizens Bank cards to a branch on Church Street in Goffstown and was told the cards had already been made "not accessible," indicating Citizens Bank had already flagged them for potential fraud.

11. Two days prior, on June 22, 2021, Citizens Bank provided Goffstown Police with supplemental documents and provided information stating the 32 cards associated with Citizens Bank were all for accounts opened on a handful of days. The accounts were all opened in either SILVA's name or in the name of a trust with SILVA listed as the trustee.

12. According to a Citizens Bank Investigator, Citizens Bank has since frozen those accounts as potentially fraudulent. The activity associated with those accounts totaled more than $400,000.

13. For example, according to subpoena returns from Citizens Bank, account number ending 3180 was under the name of Brian Allison Trust. It was opened on February 26, 2021. SILVA is listed as sole trustee on the account and SILVA signed the account opening documents.

14. I reviewed Citizens Bank records for the account ending in 3180. According to the records, a cash deposit was made on April 6, 2021, in the amount of $3,270, at a Citizens

Bank ATM on South Willow Street in Manchester, NH. I reviewed the ATM surveillance dated April 6, 2021, at 7:14 pm, and I observed SILVA and the Subject Vehicle parked in view of the ATM camera.

15. Many of the Citizens Bank accounts suspected of fraud were funded by unemployment checks from the Vermont Department of Labor. For example:

16. Account number ending 2869 was under the name of Peaceful Protesters Bail Fund Trust. It was opened on January 11, 2021. SILVA is listed as sole trustee on the account and SILVA signed the account opening documents.

17. The account was funded at least in part through Vermont unemployment checks. For example, on January 12, 2021, three unemployment checks were deposited into the account ending 2869. They were:

a. Check Number 55456, $600.00 payable to E.F.;

b. Check Number 65224, $600.00 payable to G.D.; and

c. Check Number 65231, $600.00 payable to R.C.

18. Similarly, account number ending 2931 was under the name BLM New England Trust, likely referring to the Black Lives Matter movement. It was opened on January 11, 2021. SILVA is listed as sole trustee on the account and SILVA signed the account opening documents.

19. This account was also funded in part through Vermont unemployment checks. For example, on January 12, 2021, two unemployment checks were deposited into the account ending 2931. They were:

a. Check Number 65232, $600.00 payable to V.M.; and

b. Check Number 65233, $600.00 payable to B.P.

20. Account ending 2931 was also used to make two payments to Eversource. The first was on March 16, 2021, and the second was on April 14, 2021.

21. Subpoena returns from Eversource showed that the payments were made for an Eversource account in the name "Ryan Amaro." The address associated with that account was 731 Mast Road, Floor 1 in Goffstown, New Hampshire, which appears to be the same address SILVA resided in at the time.

Fraud Involving AMEX

22. After leaving the Goffstown address, SILVA moved to the Subject Residence.

23. In August 2021, SILVA opened an account at Santander Bank in his own name and listed the Subject Residence at his address.

24. 11 Perkins Avenue in Hampton, New Hampshire, is a seven-unit building.

25. In December 2021, an investigator for American Express (AMEX) reached out to me about suspicious credit card applications submitted using Internet Protocol (IP) addresses in New Hampshire. Those applications were submitted between September 2021 and December 2021.

26. In total, these applications were for at least 15 cards in the names of at least 12 different individuals. According to subpoena returns from AMEX, the same two IP addresses were used in those applications. The IP address for applications dated on or before October 27, 2021 was 24.61.123.1. The IP address for applications dated on or after November 2, 2021 was 24.65.255.76.

27. A subpoena was issued to Comcast for information pertaining to those two IP addresses. Subpoena returns show that the subscriber of IP address 24.61.123.1 from July 3, 2021 through October 27, 2021 was M.B. The particular service address associated with IP

address 24.61.123.1 was 11 Perkins Avenue, Apt 4, Hampton, NH. M.B. paid for that Internet service. Similarly, subpoena returns show that the subscriber of IP address 24.63.255.76 from November 2, 2021 through January 4, 2022 was also M.B. The results show a service address IP address for 24.63.255.76 as 11 Perkins Avenue, Unit 2, Hampton, NH.

28. Open-source records from the New Hampshire Department of State reveal that M.B. is the registered agent of HBC Properties of Hampton, LLC, and the licensed property manager of 11 Perkins Ave, Hampton, NH. I know from my training and experience that a landlord or property manager may sometimes pay for and offer Internet service for a given property, thus providing any tenants at that property with Internet access.

29. Nine of the 15 AMEX cards associated with the applications from the IP addresses 24.61.123.1 and 24.63.255.76 listed addresses located at 11 Perkins Avenue. Again, that is a seven-unit property. However, some of the addresses listed fictional units. For example, the October 16, 2021 application for J.S. listed an address of 11 Perkins Avenue, Unit 11, Hampton, NH. No such unit exists.

30. On January 31, 2022, I spoke to the Postmaster at the Hampton, NH Post Office. The Postmaster stated all mail addressed to 11 Perkins Avenue gets deposited into one mailbox for the entire address. The Postmaster explained this is because of a high turnover rate of tenants in the area due to vacation rentals. Thus, mail addressed to imaginary units at 11 Perkins Avenue would get delivered into the same communal mailbox as mail addressed to actual units.

31. The following summarizes some evidence from law enforcement's investigation into the AMEX cards.

Victim 1 – J.F.

32. According to AMEX records, on or about September 22, 2021, an account was opened online via IP address 24.61.123.1 under the name J.F. The person opening the account used J.F.'s real name, date of birth, and Social Security number. The card issued on this account was number 376742357751000 and was mailed to 11 Perkins Avenue, Unit 2, Hampton, NH.

33. According to AMEX records, on or about October 2, 2021, a transaction for $2,019.76 was completed using card number 376742357751000 at the Wal-Mart located at 58 Plaistow Rd, Plaistow, NH. I have reviewed surveillance photos and a receipt corresponding to that purchase provided by Wal-Mart security and observed an individual matching the appearance of SILVA completing the transaction for $2,019.76.

34. According to AMEX records, on or about October 2, 2021, a transaction for $556.03 was completed using card number 376742357751000 at the Home Depot also located at 58 Plaistow Rd, Plaistow, NH. I have reviewed surveillance and a receipt corresponding to that purchase provided by Home Depot security and observed an individual matching the appearance of SILVA completing the transaction for $556.03. SILVA is using what appears to be a cellular phone while standing at the register.

35. I obtained a copy of SILVA's driver's license from the New Hampshire Department of Motor Vehicles and found that the picture on the license matches the appearance of the individual conducting the transactions at Wal-Mart and Home Depot.

36. I similarly obtained driver's license records for J.F. from the Texas Department of Motor Vehicles and determined that the picture on the license does not match the appearance of the individual conducting the transactions at Wal-Mart and Home Depot.

37. According to AMEX records, on or about November 17, 2021, a second account

was opened online via IP address 24.63.255.76 under the name J.F. The person opening the account used J.F.'s real name, date of birth, and Social Security number. The card issued on this account was number 376742685481007 and was mailed to 11 Perkins Ave, Unit 2, Hampton, NH. No successful or declined transactions were observed on this account.

38. According to AMEX records, a Massachusetts driver's license in the name J.F., number S90092427, was provided for account application verification. The picture on this driver's license matches SILVA's. The person applying for this card also needed to provide a selfie. The selfie also appears to show SILVA's face.

39. Record checks with the Massachusetts Department of Motor Vehicles on January 19, 2022 show that driver's license S90092427 belongs to D.S. D.S.'s photo does not match the appearance of the individual committing the transactions at Wal-Mart and Home Depot, and does not match the driver's license and selfie provided to AMEX.

40. On January 12, 2022, I called the real J.F. regarding the AMEX credit cards opened in his name. J.F. denied opening any of these accounts and said he did not give permission for anyone else to do so.

Victim 2 – C.R.

41. According to AMEX records, on or about September 30, 2021, an account was opened online via IP address 24.61.123.1 under the name C.R. The person opening the account used C.R.'s real name, date of birth, and Social Security number. The card issued on this account was number 376742729981004 and was mailed to 11 Perkins Avenue, Unit 2, Hampton, NH.

42. According to AMEX records, on or about November 19, 2021, a transaction for $725.00 was completed using card number 376742729981004 at the Home Depot located at 240

Lafayette Rd, Seabrook, NH. I reviewed video footage provided by Home Depot security on January 18, 2022, and observed an individual matching the appearance of SILVA completing the $725.00 transaction.

43. I obtained driver's license records for C.R. from the Oregon Department of Motor Vehicles on January 19, 2022 and determined that the picture on C.R.'s true license does not match the appearance of the individual conducting the $725.00 transaction.

44. According to AMEX records, on or about November 20, 2021, a purchase of $289.99 was completed on eBay with card number 376742729981004 from IP address 24.63.255.76. According to eBay records received on January 13, 2022, this purchase was for a set of dumbbells and shipped to C.R. at 11 Perkins Ave, Hampton, NH.

45. According to AMEX records, on or about November 16, 2021, a second account was opened online via IP address 24.63.255.76 under the name C.R. The person opening the account used C.R..'s real name, date of birth, and Social Security number. This application included a mailing address of 11 Perkins Ave, Unit 4, Hampton, NH. This application was canceled prior to card issuance.

46. According to AMEX records, on or about November 21, 2021, a purchase of $1,000 was attempted at a Victoria's Secret located in Peabody, MA using card number 376742729981004. I reviewed surveillance video from this transaction. SILVA appears on the video and is using what appears to be a cellular phone while standing at the register.

47. Additionally, AMEX records indicate a Massachusetts driver's license in the name of C.R., with license number S54092287, was submitted as supplemental information at some point during the card application processes. The subject appearing on the Massachusetts driver's license and in the photo does not match the image of either SILVA or the true C.R. A

database query of Massachusetts license number S54092287 revealed no such number exists.

48. On January 12, 2022, I called C.R. regarding the AMEX accounts opened in his name. C.R. denied opening any of these accounts and said he did not give permission for anyone else to do so.

Victim 3 – C.M.

49. According to AMEX records, on or about October 6, 2021, an account was applied for online via IP address 24.61.123.1 using C.M.'s real name, date of birth, and Social Security number. This application included a mailing address of 11 Perkins Ave, Unit 10, Hampton, NH. This application was canceled prior to card issuance.

50. According to AMEX records, on or about October 7, 2021, an account was opened online via IP address 24.61.123.1 under the name C.M. The person opening the account used C.R.'s real name, date of birth, and Social Security number. The card issued on the account was number 376742666581007 and mailed to 11 Perkins Ave, Unit 10, Hampton, NH.

51. According to AMEX records, on November 21, 2021, a transaction of $500 was successfully completed using card number 376742666581007 at a Victoria's Secret store located at 210 Andover St, Peabody, MA. I have reviewed surveillance video and a transaction receipt provided by mall security on January 6, 2022 and observed an individual matching the description of Anthony SILVA on camera completing the $500 transaction.

52. I obtained a copy of SILVA's driver's license from the New Hampshire Department of Motor Vehicles and found that the picture on the license matches the appearance of the individual conducting the transaction at Victoria's Secret.

53. I similarly obtained driver's license records for C.M. from the Louisiana Department of Motor Vehicles on January 20, 2022, and determined that the picture on that

license does not match the appearance of the individual conducting the transaction at Victoria's Secret.

54. According to AMEX records, on or about November 3, 2021, a second account was opened online via IP address 24.63.255.76 under the name C.M. The person opening the account used C.M.'s real name, date of birth, and Social Security number. The card issued on the account was number 377979719161002 and was mailed to 11 Perkins Ave, Unit 10, Hampton, NH. No successful transactions were identified on this account.

55. On January 12, 2022, I called C.M. regarding the AMEX accounts applied for in his name. C.M. said that he has never held an AMEX account in his life, and never provided permission to anyone to open an account in his name. C.M. likewise denied making any purchase for $500 at the Victoria's Secret in Peabody, MA.

56. Again, 11 Perkins Avenue in Hampton, NH is a seven-unit address. Therefore, there is no Unit 10 there.

57. On January 7, 2022, I submitted a Mail Cover for the Subject Residence. The Mail Cover lasted for a period of 30 days, or until February 5, 2022. The results of the Mail Cover showed SILVA as a person receiving mail at the Subject Residence.

58. On January 31, 2022, I spoke to the United States Postal Service Postmaster at the Hampton, NH Post Office, and he stated all mail addressed to 11 Perkins Avenue gets deposited into one communal mailbox for the entire address. The Postmaster explained this is because of high turnover in tenants in the area because the location has many vacation rentals. Therefore, even mail addressed to imaginary units at 11 Perkins Avenue would still be dropped off in the communal mailbox.

Victim 4 – C.R.2

59. As mentioned earlier, not all cards AMEX identified as fraudulent were mailed to 11 Perkins Avenue in Hampton, NH.

60. For example, according to AMEX records, on or about October 20, 2021, an account was opened online via IP address 24.61.123.1 under the name C.R.2. The person opening the account used C.R.2's real name, date of birth, and Social Security number. The card issued on this account was number 376742539521008 and was mailed to 1213 Habersham Street in Savannah, Georgia.

61. According to AMEX records, someone attempted to use AMEX credit card number 376742539521008 on 18 separate occasions at a company called Pendergrass Construction between October 27, 2021 and November 1, 2021. Only one purchase, for approximately $16,000, was approved.

62. I called and spoke with B.M., a representative of Pendergrass Construction. B.M. described herself as an administrator at the company.

63. B.M. said that the owner of the business, Amad Pendergrass, was owed money from a man named Levi Rodriguez, and that Rodriguez told Amad Pendergrass that a friend of his had given him his credit card to repay the debt. B.M. said this sounded suspicious to her and did not personally run the credit card. She recognized C.R.2's name as the one on the card Rodriguez used.

64. On January 31, 2022, I conducted surveillance of the Subject Residence. On that day, I observed SILVA driving the Subject Vehicle and park in the driveway of 11 Perkins Avenue. I further observed SILVA open the door and enter the Subject Residence.

65. On March 7, 2022, I conducted surveillance at the Subject Residence and observed the Subject Vehicle parked in the driveway of the Subject Residence.

66. On March 15, 2022, another law enforcement agent conducted surveillance at the Subject Residence and observed the Subject Vehicle parked in the driveway of the Subject Residence.

67. On March 22, 2022, I conducted surveillance at the Subject Residence and observed the Subject Vehicle parked in the driveway of the Subject Residence.

68. On March 21, 2022, a Grand Jury sitting in the District of New Hampshire returned an indictment charging SILVA with Wire Fraud, False Representation of a Social Security Number, and Aggravated Identity Theft stemming from the fraudulent obtaining and usage of AMEX credit cards.

TECHNICAL TERMS

69. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. Computer: All types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

70. As described above and in Attachments B-1 and B-2, this application seeks permission to search for records that might be found on the premises of the Subject Residence or on SILVA's person in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

71. *Probable cause.* I submit that if a computer or storage medium is found on the premises of the Subject Residence or on SILVA's person, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes

automatically downloaded into a temporary Internet directory or "cache."

72. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises of the Subject Residence or on SILVA's person because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also

falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain victims' identities, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

73. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

74. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

75. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

76. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

77. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the

device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

78. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

79. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

80. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

81. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

82. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

83. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

84. I submit that this affidavit supports probable cause for a warrant to search the Subject Residence and the person of SILVA as described in Attachments A and seize the items described in Attachments B.

Dated: March 22, 2022

Respectfully submitted,

/s/ Stephen Riggins
Stephen Riggins
Postal Inspector
United States Postal Inspection Service

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Subscribed and sworn to before me
on March 22, 2022:

/s/ Andrea K. Johnstone
Andrea K. Johnstone,
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2

Person to be searched

The person to be searched is Anthony Silva (DOB [redacted]1984), who resides at 11 Perkins Ave, Unit 1, Hampton, New Hampshire, 03842

ATTACHMENT B-2

Property to be seized from Anthony Silva

1. All records relating to violations of 18 U.S.C. § 1344 (Bank Fraud); 18 U.S.C. § 1343 (Wire Fraud); 42 U.S.C. § 408(a)(7)(B) (False Representation of a Social Security Number); or 18 U.S.C. § 1028A (Aggravated Identity Theft); and associated conspiracies (collectively the "Subject Offenses"), those violations involving Anthony Silva or his accomplices/co-conspirators, and occurring after 2020, including:

   a. Records, communications, and information relating to possible identity theft victims;

   b. Records, communications, and information relating to the use of aliases;

   c. Credit cards and/or gift cards;

   d. Credit card receipts;

   e. Bank, financial, credit card, and investment account records showing the ownership, control, amounts, locations, and disposition of funds held by Anthony Silva or his accomplices and co-conspirators;

   f. Records and information relating to the identity, locations, and activities of Anthony Silva or his accomplices and co-conspirators; and

   g. Records or information relating to the occupancy or ownership of 11 Perkins Ave, Unit 1, Hampton, New Hampshire, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Computers or storage media used as a means to commit the Subject Offenses, including mobile devices such as laptops and smart phones.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Device Unlock: During the execution of the search of Anthony Silva described in Attachment A-2, law enforcement personnel are authorized to:

a. Press or swipe the fingers (including thumbs) of Anthony Silva to the fingerprint scanner of the device(s); and/or

b. Hold the device(s) in front of the face of Anthony Silva and activate the facial recognition feature;

for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.